THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

JUN 2 2005

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Investment Review Process Overview and Concept for Operations for Investment Review Boards

In accordance with the Deputy Secretary of Defense memorandum, March 19, 2005, subject: "Delegation of Authority and Direction to Establish and Investment Review Process for Defense Business Systems," the attached Investment Review Process and Concept for Operations for Investment Review Boards is approved and effective immediately. This new process replaces existing domain and BMMP certification processes for all business system modernization investment review effective immediately.

Michael W. Wynne
Vice-Chairman of the Defense Business
Systems Management Committee

Attachment:
As stated

DISTRIBUTION:
DEPUTY SECRETARY OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARMENT OF DEFENSE
ASSISTANT TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Investment Review Process Overview

And Concept of Operations For Investment Review Boards

May 17, 2005

Department of Defense

TABLE OF CONTENTS

1.0 PURPOSE

The Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2005 states that funds appropriated to the Department of Defense (DoD) may not be obligated for a defense business system modernization that will have a total cost in excess of $1M unless—

1) the approval authority designated for the defense business system certifies to the Defense Business Systems Management Committee that the business system modernization is in compliance with the enterprise architecture; is necessary to achieve a critical national security capability or address a critical requirement in an area such security or safety; or is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration alternative solutions;
2) the certification by the approval authority is approved by the Defense Business Systems Management Committee.

The Secretary of Defense has delegated responsibility and accountability for review, approval, oversight of the planning, design, acquisition, deployment, operation, maintenance, and modernization of defense business systems to Approval Authorities. The Approval Authorities, who are referred to in this document as Certification Authorities, are the Under Secretary of Defense for Acquisition, Technology and Logistics, Under Secretary of Defense (Comptroller), Under Secretary of Defense for Personnel and Readiness, and the Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer of the Department of Defense.

This document integrates the policies, specifies responsibilities, and identifies the processes to establish and operate Investment Review Boards (IRBs) for the purpose of reviewing all business system investments, at least annually, and for certifying business system modernizations/enhancements over $1M as required by 10 U. S. C. 2222 (a) (1). It provides policies to ensure consistent implementation of 10 U. S .C. 2222 within the Department of Defense (DoD).

This document outlines the Investment Review Board process for certification of defense business system modernization. It will be followed by all IRB members, Component Headquarter staffs, Chief Information Officers (CIOs) and Program Managers (PMs) who have responsibility for business systems investments. This document elaborates on applicable regulations, defines governance, roles and responsibilities, certification criteria, required reports, processes and controls, and includes samples of: IRB charters, certification submission templates, and other documents (Appendices A-D). Upon reading this document, PMs, Component and DoD Enterprise Portfolio Managers, and IRB chairs and members should understand the following.

- Why IRBs were established,
- Who must comply with and use this process,

- When an IRB review and certification is required,
- What governance, roles, information requirements, and products are associated with the IRB review and certification processes,
- How the IRB review aligns to DoD 5000 series Joint Capability Interoperability Development System (JCIDS) and requirements processes,
- How the DoD and Component business enterprise architectures support the IRB review process,
- How to prepare for an IRB review,
- How to operate an IRB,
- How to use the IRB review process

2.0 SCOPE

This document contains policies to be followed by Office of the Secretary of Defense (OSD) managed IRBs. It describes how these processes will interface with the military departments, DoD agencies, the Joint Staff and combatant commands, hereafter referred to as Components. It does not prescribe Component IRB processes and business system investment procedures. However, Components are expected to establish their own IRB processes to manage their business systems transformation activities, and to ensure NDAA compliance. Those processes and procedures should be consistent with applicable laws, regulations and this guidance.

Certifications must be done for business system modernizations and enhancements that will have a total cost in excess of $1M, and for modernizations and enhancements to systems or in lines of business that are designated as OSD Items of Interest. The $1M total cost threshold only includes funds used to acquire or develop a new defense business system, or to modify or enhance an existing defense business system. Funds necessary to maintain current services are not included.

OSD Investment Reviews will leverage OMB Exhibit 300 reports as well as existing MAIS processes.

3.0 OPERATING PRINCIPLES AND OBJECTIVES

IRBs are expected to perform business system investment reviews as expeditiously as possible to provide rapid delivery of critical capabilities to support the warfighter. They are expected to:

- Ensure business capabilities are delivered that support the warfighting mission
- Enable transformation by ensuring investments align with DoD strategic mission, goals and objectives and with Core Business Mission (CBM) capabilities
- Enhance compliance with the DoD Business Enterprise Architecture
- Exploit common processes
- Ensure an appropriate level of review based on cost, scope, and complexity

- Comply with the legislation, regulations, policies and procedures outlined in this document and others as appropriate

4.0 BACKGROUND

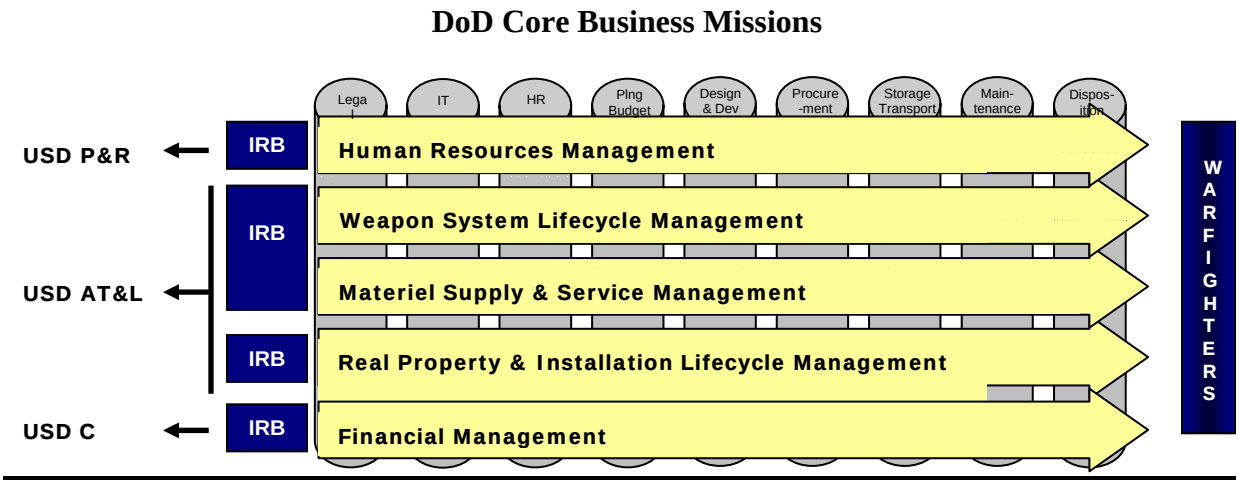
In July 2001, the Financial Management Modernization Program (FMMP) was established by the Secretary of Defense (SECDEF) to modernize DoD business operations and systems. The program was renamed Business Management Modernization Program (BMMP) in May 2003 to reflect the Department's focus on transforming the Department's business processes. Transformation objectives reported in the March 2005 report to Congress included:

- To define the future capabilities necessary to support the Warfighter, and focus the activity of business systems modernization on acquiring those capabilities
- To define and declare capabilities that should be common throughout the DoD business enterprise and direct the implementation of enterprise-wide systems with greater visibility at the highest levels of leadership within the Department
- To control current and future investments in business systems, through the governance of the Defense Business Systems Management Committee (DBSMC) and IRBs

The NDAA of FY 2005 prescribes the establishment of IRBs and the DBSMC to certify and approve defense business system modernization/enhancement investments over $1M and to review all business system investments at least annually. It requires the DBSMC to develop a transition plan and an enterprise architecture sufficiently defined to guide, constrain and permit implementation of interoperable defense business system solutions. It also requires SECDEF to provide to Congress information about all business systems, reviews, certifications, status of NDAA compliance, and improvements in business operations.

In order to ensure compliance with the NDAA and to create strategic alignment between the Department's mission, goals and objectives and its business processes and systems, the SECDEF established the following CBM strategic capabilities and assigned responsibility for implementing these capabilities to the following principal staff assistants (PSAs):

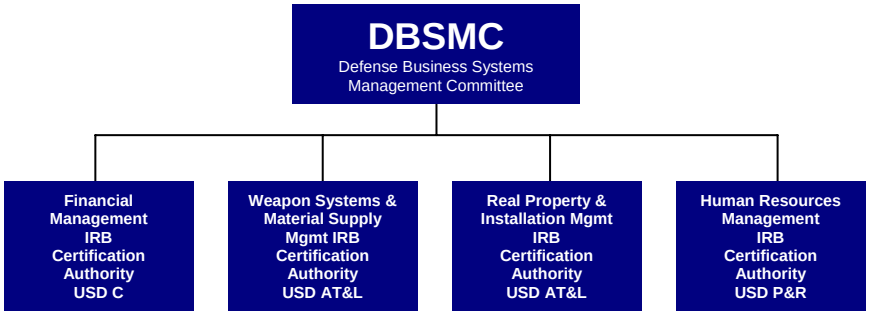
- Financial Management (FM) – USD(C)
- Human Resources Management (HRM) – USD(P&R)
- Real Property and Installations Lifecycle Management – USD(AT&L)
- Weapon System Lifecycle Management (WSLM) – USD(AT&L)
- Material Supply and Service Management (MSSM) – USD(AT&L)



5.0 GOVERNANCE

The FY 2005 NDAA establishes a governance organization that reports to the Deputy Secretary of Defense (DEPSECDEF). This organization has responsibility for reviewing the planning, design, acquisition, development, deployment, operation, maintenance, modernization and project cost benefits and risks of defense business systems investments of more than $1M.

This new governance organization is illustrated and described below.



5.1 THE DEFENSE BUSINESS SYSTEMS MANAGEMENT COMMITTEE (DBSMC)

The DBSMC is chaired by the DEPSECDEF, or the vice-chair in his absence, and is responsible for approving business systems modernization investments in excess of $1M which have been certified under 10 U. S .C. 2222 (a) (1) by designated certification authorities. Its membership includes:

- Deputy Secretary of Defense (Chair);
- Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) (Vice Chair);
- Secretaries of the Military Departments and the heads of the Defense Agencies;
- Under Secretary of Defense (Comptroller) (USD(C));
- Under Secretary of Defense for Personnel and Readiness (USD (P&R));
- Vice Chairman of the Joint Chiefs of Staff (JCS);
- Commander, U.S. Transportation Command (TRANSCOM);
- Commander, U.S. Joint Forces Command (JFCOM);
- Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII/CIO)); and
- Director, Program Analysis and Evaluation (PA&E) (Advisory).

5.2 OFFICE OF SECRETARY OF DEFENSE (OSD) CERTIFICATION AUTHORITIES (CA)

SECDEF has assigned accountability for business activities, and the systems that support them, to the following principal staff assistants who, in addition to their other responsibilities, are certification authorities:

- The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) – for acquisition, logistics, installation and environment activities
- The Under Secretary of Defense (Comptroller) (USD(C)) – for financial management activities
- The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) – for human resource management activities
- The Assistant Secretary of Defense (NII) and (CIO) of DoD – for information technology infrastructure and information assurance activities
- The Deputy Secretary of Defense - for DoD business activities not addressed above

5.3 OSD INVESTMENT REVIEW BOARDS (IRBS)

Per the NDAA and the Deputy Secretary's March 19, 2005 memorandum, each of the CAs above is required to establish and charter an IRB to provide oversight over IR processes for business systems supporting activities under its designated area of responsibility. A sample IRB charter format is attached (Appendix A). Standard operating procedures and guidelines for all IRBs are described in this document and will be implemented across all IRBs to ensure consistency. Exceptions must be approved by the DBSMC. IRBs are to include representatives from combatant commands (COCOMS), the Components, and the Joint Chiefs of Staff who will participate in reviews as appropriate based on the types of business activities and systems being reviewed and certified.

5.4 COMPONENT LEVEL PRE-CERTIFICATION AUTHORITIES (PCAS)

Consistent with section 11312 of title 40, the Components are expected to establish their own investment review governance structures and pre-certification authorities to support their transformation initiatives.

6.0 ROLES & RESPONSIBILITIES

6.1 DEFENSE BUSINESS SYSTEMS MANAGEMENT COMMITTEE

The DBSMC will meet quarterly, but other meetings may be called at the direction of the chair. The DBSMC coordinates defense business system modernization initiatives and is responsible for recommending to the Secretary of Defense policies and procedures necessary to effectively integrate the requirements of the NDAA into all business activities and transformation, reform, reorganization or process; review and approve any major update of the defense business enterprise architecture; and managing cross-business mission area integration consistent with the enterprise architecture.

To meet these responsibilities, the DBSMC will coordinate activities required to :

- Establishing strategic direction and plans for the Business Mission Area (BMA)
- Ensuring BMA efforts enable cross-Department, end-to-end interoperability
- Approving metrics and targets for tracking of business systems transformation progress
- Approving the BMA Strategic Plan, overall Business Enterprise Architecture, and the transformation program baseline
- Approving certification by Approval Authorities
- Complying with all public laws and annual reporting requirements and addressing all concerns of oversight bodies
- Addressing escalation issues
- Ensuring investment review criteria to measure business mission benefit are consistent across IRBs and leverage existing Capital Investment Report (Exhibit 300) information
- Ensuring all IRBs provide consistent guidance to Component Pre-Certification Authorities

6.2 OSD CERTIFICATION AUTHORITIES (CA)

OSD Certification Authorities are assigned responsibility, within their core business mission areas, for enterprise level-architecture products, portfolio management governance, and transition planning, conducting business system investment reviews, and certifying business system modernization and enhancements. With respect to the IRB process, each CA is responsible for:

- Providing leadership for business system investments associated with that core business mission area

- Establishing, chartering, designating members and standing-up an IRB to review systems for which he/she are assigned responsibility
- Assuming responsibility for the review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance and modernization of the defense business systems assigned to them
- Advocating DoD Business Enterprise capabilities and DoD Enterprise Systems where appropriate to support the warfighting mission.
- Establishing priorities and strategic direction for the business systems review
- Reviewing certification packages assigned to the business area and making certification decisions
- Approving Core Mission Area transition plans
- Determining the appropriate level of review based on the cost, scope, complexity and risk associated with the investment
- Identifying specific systems or specific lines of business as "CA interest" and requiring review for systems that support those lines of business.
- Ensuring compliance with the references listed below and the guidance in this document
- Ensure timely coordination with other Pre-Certification and Certifications Authorities, as appropriate on cross-cutting initiatives
- Reporting CA certification decisions to all the OSD-level IRBs and to the DBSMC

6.3 OSD INVESTMENT REVIEW BOARDS (IRBS)

The IRB chairs are responsible for:

- Presiding at IRB meetings
- Appointing additional members to the IRB as appropriate
- Coordinating with other IRBs, as required, for systems that perform multiple functions and cross business mission areas
- Ensuring participation on other IRBs as members when designated
- Adhering to the standard processes and procedures that apply to all IRBs
- Leading the establishment of specific core business mission area criteria for business system certification. These criteria are business-focused metrics reflecting tangible end-to-end business mission improvements that clearly benefit the warfighting mission of the department.
- Providing clear and concise documented guidance to the Component Pre-Certification Authorities, enabling Component pre-certification.

The IRBs are responsible for:

- Ensuring review of every business system modernization/enhancement investment at least annually
- Performing the appropriate level of review using a "Tiered Process" which links level of review to scope, complexity, cost, and risk
- Reviewing and approving the enterprise criteria

- Assessing whether business system investments are consistent with the Department's requirements based on:
  - Essentiality -- whether it achieves an essential capability
  - Alignment with DoD strategic mission, goals and objectives
  - Beneficial impact in terms of the criteria defined for the IRB's core business mission area that justifies the system investment
- Recommending to the CA certification or non-certification based on certification criteria (Appendix E).

6.4 COMPONENT DESIGNATED PRE-CERTIFICATION AUTHORITIES (PCAS)

Each Component and COCOM is responsible for designating headquarters level approval authorities who are assigned accountability for business systems investments. The military departments may decide to designate a single PCA for all business systems or they may designate different PCAs for different business mission areas. In no case should there be more than one PCA per Service, per core business mission area. Component PCAs are responsible for:

- Acting as the Pre-Certification Authority for business systems modernization/enhancement investments over $1M and submitting requests to the CA IRB for certification of business system investments over $1M.
- Maintaining Component architectures that are compliant with the Global Information Grid (GIG) (the business component of the GIG is the DoD Business Enterprise Architecture (BEA)) and the DoD Architecture Framework (DODAF).
- Participating in OSD level IRBs as designated members if appointed
- Designating the office and person at the headquarters level who is responsible for system reviews, and compliance with the NDAA. A copy of the designation letter for headquarters level PCAs is to be provided to the DBSMC chair annually or whenever there is a change to the office or representative (Appendix B)
- Establishing the Component's own investment review processes and governance structure (consistent with section 11312 of title 40) to support Component transformation initiatives
- Ensuring that reporting reflects "capabilities-based" management with a level of detail consistent with IT budget reporting to OMB
- Integrating DoD's certification criteria with Component certification criteria for modernizations over $1M
- Integrating Component processes with the OSD's processes established in this document
- Conducting Component level reviews of certification information (Appendices C-D) to the single entry point for systems requiring CA/DBSMC certification and approval
- Providing to IRB/CA/DBSMC, as applicable, regular updates on business systems that have been reviewed, their status and, on an annual basis, providing a consolidated report
- Ensuring information is current and correct in the official DoD business system repository

6.5 INFORMATION TECHNOLOGY (IT) BUSINESS SYSTEM PROGRAM MANAGERS (PMS)

All business system PMs must understand that their systems are subject to annual reviews and certification by multiple levels of authorities to include the Component portfolio manager, the Component PCA, the appropriate OSD level IRB and the DBSMC. Approval must be granted by the DBSMC for any program that wishes to obligate more than $1M. Beginning October 1, 2005, failure to do so will be a violation of section 1341(a)(1)(A) of title 31 (The Anti-Deficiency Act).

Specifically, PMs are responsible for:

- Ensuring program information is accurate and current in mandatory DoD level business system repositories as required by NII policy, or the appropriate Component-level tool set used to populate that repository
- Verifying that the IRB certifying authority and DBSMC, via the appropriate headquarters level authority, have completed system review, certification, and approval before obligating funds over $1M for modernization
- Ensuring information contained in the DoD business system repository, or the appropriate Component-level tool set is current, complete and accurate

7.0 INVESTMENT REVIEW BOARD PROCESS

The investment review process is separated into the following sections:

- Determination of requirement for review and certification
- Program Manager preparation
- Component review and pre-certification
- OSD level review and certification

7.1 DETERMINATION OF REQUIREMENT FOR REVIEW AND CERTIFICATION

All DoD and business systems modernization investments must be reviewed at least annually. Who performs the review, and the level of review performed, varies and is identified in this document.

A defense business system is:

An information system, other than a national security system, operated by, for, or on behalf of, the DoD including: financial systems, mixed systems, financial data feeder systems and information technology and information assurance infrastructure, used to support business activities such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment and human resources management. (10 U. S. C. 2222 (j) (2))

(Information technology and information assurance infrastructure systems that generally support the DoD Enterprise and all GIG users are not classified as defense business systems and belong in the Enterprise Information Environment Mission Area.)

A defense business system modernization is:

The acquisition or development of a new defense business system; or any significant modification or enhancement of existing defense business systems (other than necessary to maintain current services). (10 U. S. C. 2222 (j) (3))

Systems with total modernization expenditures under $1M do not require an OSD level IRB review, certification or DBSMC approval unless the system or the line of business which it supports has been designated as special interest by the CA.

The matrix below summarizes the levels of review required for business system investments based on specific criteria. It also assigns specific responsibilities to the Components, IRBs/CA and DBSMC as follows:

- Pre-certification for investments of $1M and over – Component PCA
- Certification of investments $1M and over – CA
- Certification of investments for special interest – CA
- Approval/disapproval of certifications of investments $1M and over – DBSMC

IRB Review and Approval Matrix for Business System Modernization Investments

	TIER 3 **Modernization/Investment** **Greater than $1M* to less than $10M** **Note [1]: If a delegated (i.e., ACAT IAC), program, Tier 2 applies**	TIER 2 **Modernization/Investment** **$10M* to less than MAIS Threshold** (Currently $32M) **or CA Interest[1] or Enterprise Level [1]** NOTE[1]: If ACAT IAM or 1AD, Tier 1 applies	TIER 1 **Systems designated as** **ACAT IAM ACAT IAD, and ACAT 1C**
Component PCA – Pre-Certification	**Reviews and pre-certifies each system or bundle of systems as compliant. Submits certification package to OSD Single Entry Point.**	**Reviews and pre-certifies each system or bundle of systems as compliant. Submits certification package to OSD Single Entry Point.**	**Reviews and pre-certifies each system or system-of-systems as compliant. Participates in acquisition management process. Submits certification package to OSD Single Entry Point.**

OSD Single Entry Point POC	**Works with IRB Chairs to determine the appropriate IRB(s) for packages which do not specify a core business mission area.** **Manage DBSMC appeals and feedback.**	**Works with IRB Chairs to determine the appropriate IRB(s) for packages which do not specify a core business mission area.** **Manage DBSMC appeals and feedback.**	**Works with IRB Chairs to determine the appropriate IRB(s) for packages which do not specify a core business mission area.** **Manage DBSMC appeals and feedback.**
IRB and CA (PSA) Recommend and Certify	**IRB recommends to the CA who certifies to the DBSMC based on:** **Component pre-certification and enterprise capability impact(s).**	**IRB recommends to the CA who certifies to the DBSMC based on:** **Component pre-certification and analysis of the business case (See section 7.4.2)**	**IRB recommends to the CA who certifies to the DBSMC based on:** **Participation in pre/milestone meetings and reviews of documentation/letters produced by JCIDS and DAS processes (See section 7.4.2)**
DBSMC Approve	**Approves certification**	**Approves certification**	**Approves certification**

*** An ACAT IAM program is defined in DoDI 5000.2 as either: (1) MAIS: Dollar value of AIS estimated by the DoD Component Head to require program costs (all appropriations) in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life-cycle costs in excess of $378 million in FY 2000 constant dollars; or (2) MDA designation as special interest. An ACAT IAD program is defined in DoDI 5000.2 as either: (1) MDAP: Dollar value: estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than $365, or (2) MDA designation MDA designation as special interest. In the event that these definitions change in DoDI 5000.2, the definitions of ACAT IAM program and ACAT ID program in this document shall be the definition in the most current version of DoDI 5000.2.*

7.2 PRE-CERTIFICATION AUTHORITY (PCA) PREPARATION

Pre-Certification Authority (PCAs) are required to comply with investment review policies prescribed by the Component and by OSD. Component level requirements are not addressed in this document. The focus of this document is principally on OSD level investment review requirements, but it also defines the information exchanges and touch points between the Component and the OSD level business system investment review processes. PCAs are required to:

- Update the official DoD business system repository, thirty days prior to submitting a certification package
- PCA designees submit certification packages to the designated single entry point

Within the DoD business system repository the PCAs will be required to identify systems as: core, interim, or legacy. Core systems are typically new systems that are part of the target architecture and usually require the highest level of review because they are the focus of the Department's end state. Interim systems are existing or emerging systems that may be modernized to provide interim capability until replaced by core systems. Legacy systems are existing systems flagged for retirement due to redundancy or obsolescence.

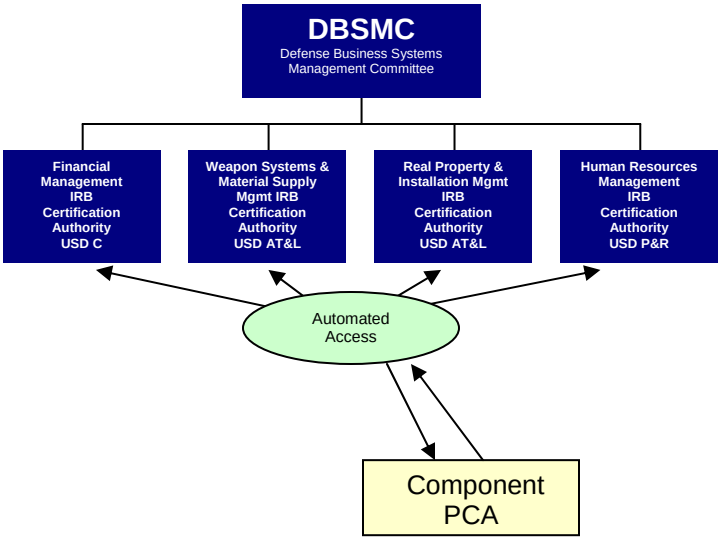
7.3 COMPONENT LEVEL REVIEW AND PRE-CERTIFICATION

For business systems modernization/enhancement requests greater than $1M, PCAs must "pre-certify" the modernization request based on established criteria before forwarding to the OSD single entry point.

Completed business systems modernization/enhancement certifications for investments greater than $1M or of CA interest are to be forwarded electronically to the single automated repository. The certification package should contain:

- The PCA's responses to certification criteria
- Economic viability analysis used by Components
- The Component pre-certification compliance letter (Appendix D)
- POC information for the Component PCA

SYSTEMS CERTIFICATION AND APPROVAL PATH



The DBSMC approves all system modernization/enhancements over $1M.

There are 4 IRBs, each chartered by an Approval Authority designated by SECDEF. Each CA certifies systems and forwards approved certification packages to the DBSMC for approval. Systems that cross business mission areas will be assigned to a lead CA/IRB.

The automated workflow tool will provide access to certification packages for the appropriate IRB to download.

The designated Component PCA, will review PM submissions against the Transition Plan to determine whether it should be approved based on Component and OSD criteria. PCAs will record their review results and forward to the OSD single entry point via the DoD automated workflow tool when completed or return to the PM for disapprovals or investments under $1M.

Whenever possible, Components are encouraged to submit "capability based" portfolios of systems -- meaning, all systems support a single capability or an interrelated set of capabilities – in order to facilitate effective and efficient review, and to ensure delivery of desired capabilities.

7.4 OSD LEVEL REVIEW AND CERTIFICATION PROCESSES

Once a package is sent from the Component PCA and received by the appropriate OSD CA and applicable IRB members, the following steps will be followed:

- OSD level IRB review and certification
- IRB evaluation DBSMC approval, disapproval, escalation and notification

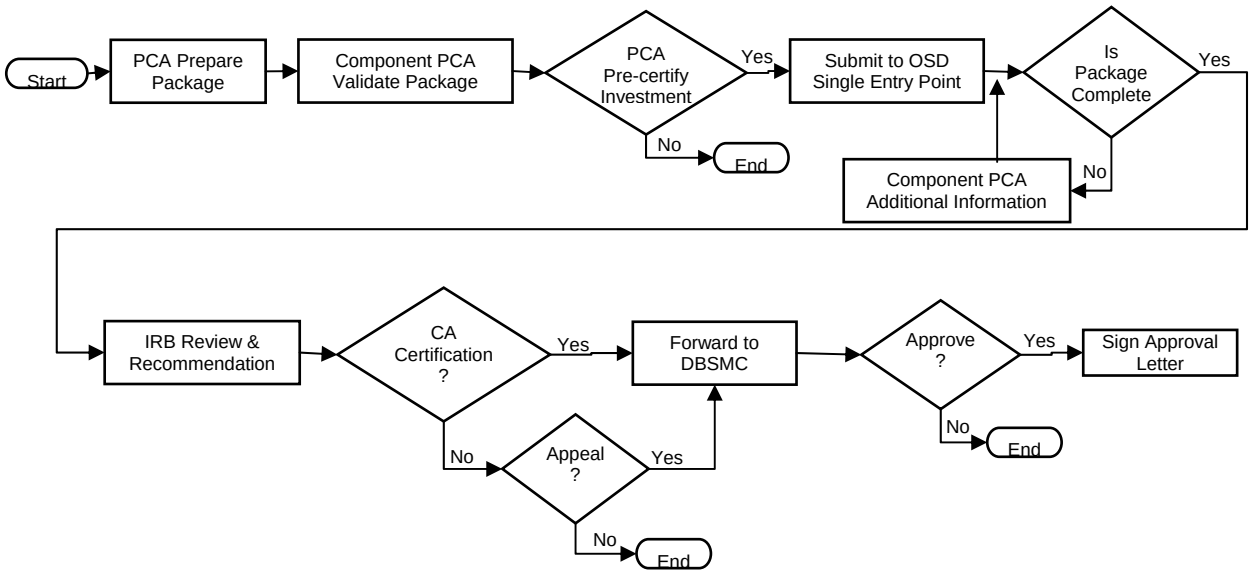
7.4.1 OSD Level IRB Review and Certification

As described above, there are three different levels of certification review, or Tiers, which are established based on specific criteria to include: the dollar value of the modernization/enhancement (for existing systems) or for the program (new systems or systems under development), whether the program has been designated as a "CA interest" program

(regardless of dollar value) or whether it meets the criteria for Acquisition Category I. Each Tier is discussed below beginning with Tier 3.

Tier 3 (Modernizations greater than $1M but less than $10M) and **Tier 2** (Modernizations of $10M up to the MAIS threshold) follow the process described below:

TIER 2-3 BUSINESS SYSTEM IRB PROCESS



Component PCA

- If the modernization is over $1M, makes a pre-certification decision and, if compliant, prepares a pre-certification letter **(Appendix D)** to the appropriate OSD level CA IRB
- Forwards PM package with cover letter to the OSD single entry point

OSD Level CA IRB

- Reviews submission package and verifies completeness
- Determines Tier level
- Reviews package
- IRB makes a certification recommendation to CA
- CA certifies and forwards to DBSMC or disapproves and notifies all IRB members

DBSMC

- Approves CA certifications and documents in letter

*NOTE: DoD Enterprise Business Systems and CA Interest programs normally follow the **Tier 2** certification process unless they are designated as MAIS (ACAT IAM) or ACAT IAD; in which case, they will follow the* **Tier 1** *process below.*

Tier 1 reviews apply only to business system programs designated as ACAT IAM and IAD. (See DoD Instruction 5000.2 and the footnote to the table in section 7.1 for the definitions of these terms.) **Tier 1** business systems will leverage the Defense Acquisition process and Joint Capabilities Integration Development System (JCIDS) requirements generation processes to meet their certification requirements.

Designated representatives from the IRB/CAs will participate in these reviews to include:

- Milestone Decision Authority (MDA)
- Joint Staff JCIDS
- Functional Capabilities Board (FCB) - IRB representatives can ask requirements based questions relevant to the IRB but not necessarily important to the FCB

Additionally these programs must prepare critical acquisition documents which must be made available to IRB members to include:

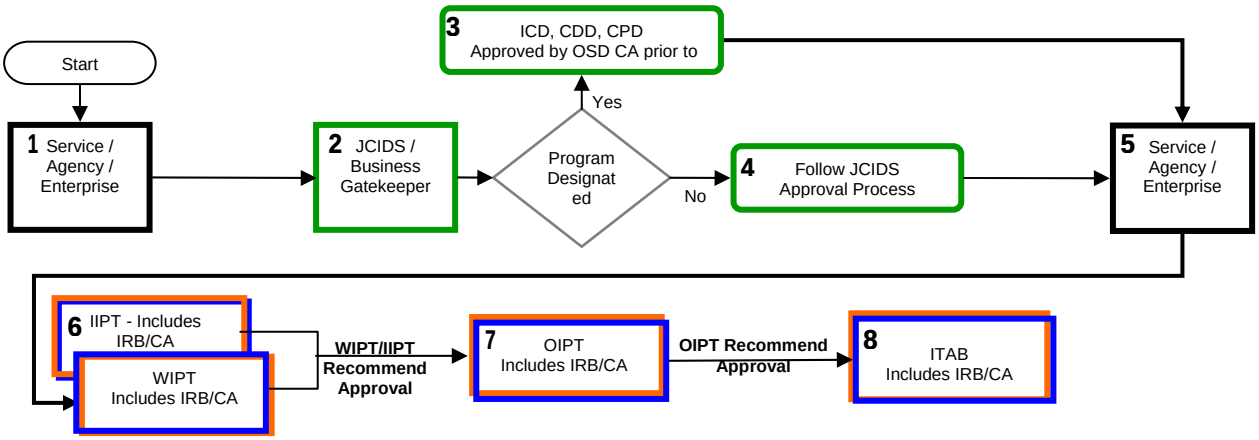
- Initial Capabilities Document (ICD)
- Capability Development Document (CDD)
- Capabilities Production Document (CPD)
- Acquisition Strategy

To integrate these two processes, representatives from the OSD level CAs, IRBs, or their support personnel must attend various acquisition meetings and raise and resolve issues relative to the management of the business system under consideration. Such meetings include:

- The Integrating Process Team (IPT) meetings
- Applicable Working Level IPTs (as required)
- IPTs relating to JCIDS
- Overarching IPTs to develop recommendation for a milestone decision and resolve any issues, including those to ensure compliance with IRB criteria

The **Tier 1** process applies to the years in which there are milestone reviews. In those years in which no milestone review is scheduled, the annual requirement for a system review still applies and an abbreviated version of the standard review process (IRB Review Criteria and economic viability analysis, but not Acquisition documents) used by Tiers 2 and 3 will be followed. The IRB or the CA may decide, in appropriate cases, to use the Defense Acquisition Executive Summary (DAES) process as the basis for the annual review. All waivers and rationale must be reported in the SECDEF's annual report to Congress.

TIER 1 - CERTIFICATION & APPROVAL PROCESS FOR ACAT I AM & ACAT IAD BUSINESS SYSTEM ACQUISITIONS



1. DoD Components will collaborate with the sponsoring OSD CA in the development of requirements documents (Integrated Capabilities Document, Capabilities Development Document, and Capabilities Production Document).
2. The documents will be submitted to the JCIDS/Business Gatekeeper to obtain a determination as to whether the Joint Staff will designate the program "Independent."
3. **If designated Independent, the CA will approve all requirements documents**. This may require IRB or DBSMC meetings, as the OSD CA sees fit.
4. If the program is designated Joint Interest or JROC Interest, the JCIDS Gatekeeper will assign the program to a Functional Capabilities Board (FCB). OSD CA/IRB representatives will actively participate in FCB discussions leading to Joint Staff approval of requirements documents. (See CJCSI 3170.1f for details of the JCIDS process.)
5. The Program Manager (PM) will support the Component sponsor and collaborate with the sponsoring OSD CA in development of the requirements documents and be responsible for preparation of all required acquisition decision support documentation. That documentation will support and establish the readiness of a program to proceed through the acquisition process.
6. The PM will establish Integrated Product Teams (IPTs) to develop and coordinate the required documentation. OSD CA/IRB representatives will participate in IPT discussions in preparation for an acquisition decision. Issues relative to unique OSD CA/IRB information requirements and all other program issues will be resolved via the IPT process. (For a description of the IPT process, see the Defense Acquisition Guidebook at http://akss.dau.mil/dag/.)
7. When the PM, in coordination with the IPT membership, determines that the program is ready for an acquisition decision, the program will be presented to the Overarching IPT (OIPT) for review. The purpose of the OIPT is to review the program, resolve issues and assess readiness for Milestone Decision Authority (MDA) decision. The OIPT membership will include principals from the OSD CA/IRB organization. On completion of OIPT deliberations, the OSD CA/IRB principal will reflect OSD CA certification by coordinating on the OIPT Report.
8. OIPT leadership will schedule the program for an ITAB review. The MDA, based on the advice of the ITAB members, will decide if the program is ready to proceed to the next phase of the acquisition process. The MDA decision will be reflected in the Acquisition Decision Memorandum (ADM). The ITAB membership will include the DBSMC members. The ADM will be coordinated with all ITAB members. The coordinated ADM will constitute DBSMC approval as required by the NDAA. A DBSMC member may appeal unresolved issues to the DBSMC chair.

7.4.2 Investment Review Board Evaluation

The IRB will review and recommend decisions on all requests for certification. This may be done through paper coordination or through meetings. If any issues arise during coordination, the IRB Chair will determine if a meeting is needed to address the issues. If it is determined that an IRB meeting is warranted, the IRB chair will determine the format and structure for the review and identify required attendees.

For certifications that require coordination with other IRBs, it is the responsibility of the Lead IRB to ensure that all information is provided to all interested IRBs. The interested IRBs must participate in the review with the Lead IRB to avoid duplicative reviews of the same request.

The IRB chair will determine the structure required for meetings and participation from the Component Pre-Certification Authority and other IRBs. Programs that cross business missions will use an IPT-like structure and representatives from all CBM IRBs will be invited to participate in review activities. Actual participation is discretionary. Usually, the responsible PCA, budget personnel, and systems engineer/architect will be asked to attend. Component attendees will be determined by the type(s) of systems being reviewed. For example, a review of an inventory management system would include the Defense Logistics Agency; a transportation system would include USTRANSCOM, etc.

7.4.3 DBSMC Approval, Disapproval, Escalation, Notification and Appeal

The CA will submit the certification results to the Vice Chair of the DBSMC and IRB members. The entire DBSMC membership will be notified of all CA certification decisions. Principal members and associate members within the DBSMC have five business days to object to the decision, and appeal to the DBSMC for a review of the decision. Rationale for the objection must be provided in writing and must present a strong case for the decision review.

If no objections are raised, DBSMC members will approve CA recommendations, and the DBSMC approval recommendation will be forwarded to the DBSMC Chair (or designee)for signature. The date the approval letter is signed becomes the official approval date and will be recorded in the DITPR by the appropriate support personnel.

In cases where an IRB disapproves a certification, the certification process will end and the Component will be notified.

Notification of decisions will be provided to the Component. Components will ensure Program Managers are notified when the DBSMC approves or disapproves certification.

8.0 ANNUAL REPORTS

The SECDEF is required to submit annual reports to Congress on business systems modernizations and business systems investments reviews. IRBs will submit annual reports to the DBSMC Vice Chair for consolidation and approval prior to forwarding to the SECDEF.

9.0 DOCUMENTATION, REPORTS, DATA REPOSITORY AND AUTOMATED TOOL

The following table summarizes the documents, reports, data repository and tool updates generated by various stakeholders and used in the investment review process. They are:

SYSTEM REVIEW AND CERTIFICATION DOCUMENTATION AND TOOLS

Responsibility	Documents	System/Tool Updates
Component – Tier 2-3 systems	• Prepare and submit OSD required certification package to include: certification questionnaire, economic viability analysis prepared by Component or independent cost review authority • Component Pre-Certification letter	• Update data repository with systems information OR provide systems information to the Component PCA to perform update • Input certification submission package into the system certification repository
Component – Tier 1 programs	Same as above in non-milestone review years or, in milestone review years: • Required Acquisition Documents *NOTE: May substitute acquisition documents that provide if comparable information whenever available*	• Update data repository with systems information OR provide systems information to the Component PCA to perform update • Input certification submission package into the system certification repository
Component	• Pre-certification recommendation letters for systems $1M and over	• Submit pre-certification letter via the system certification repository • Update data repository with systems information
CA/IRB	• Prepare certification summary reports • Document IRB proceedings and voting results	• Update/monitor system certification tool with IRB/DBSMC results • Update data repository with certification and approval results and dates
DBSMC	• Review and Approve Annual Reports to Congress • Sign Authority to Obligate funds letter	
SECDEF	• Letter to Congress with annual business system investment review and compliance information **(See section 8.0)**	

10.0 REFERENCES

- Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Section 332 which enacted 10 U. S. C. 2222.
- Section 8083 (b) of the National Defense Appropriations Act, 2005
- Section 11312 of title 40, United States Code
- Office of Management and Budget (OMB) Circular A-130 (Management of Federal Information Resources)
- Assistant Secretary of Defense Memorandum, "Information Technology Portfolio Management," March 22, 2004
- Assistant Secretary of Defense Memorandum, "Department of Defense (DoD) Information Technology Portfolio Registry (DITPR)," March 17, 2005
- DoDD 8100.1, September 19, 2002, Global Information Grid (GIG) Overarching Policy
- DoDD 4630.5, May 5, 2004, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

- DoDD 8320.2, December 2, 2004, Data Sharing in a Net-Centric Department of Defense

11.0 KEY DEFINITIONS

Term	Definition
ACAT IA	Programs which are Major Automated Information Systems (MAIS) or programs designated by ASD (NII) to be ACAT IA. The Milestone Decision Authority is the DoD CIO.
ACAT IAM	Is a sub-category of ACAT IA and is a program for which the Milestone Decision Authority (MDA) is the DoD Chief Information Officer (CIO)
ACAT IAD	A MDA designated special interest program or a program that will require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than $365M
Application	A software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges.
Automated Information System (AIS) Application	For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in DODD 5000.1, "The Defense Acquisition System," May 12, 2003; Certified Current as of November 24, 2003. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000; however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System.**
Below Major Command	Systems which are not DoD-wide, Joint, Multi-, Standard Systems or Major Command Standard systems. Includes bridges (systems that interface between two or more other systems), uniques, and systems used at a single site.
Bridge	Systems that interface between two or more other systems.
Business Capability	The ability to execute a specific course of action. It can be a single business enabler or a combination of business enablers (e.g. business processes, policies, people, tools or systems, information) that assists

Term	Definition
	an organization in delivering value to its customer.
Business Enterprise Architecture	The Business Enterprise Architecture (BEA) is a blueprint to guide and constrain investments in DoD organization, operations, and systems as they relate to or impact business operations. It will provide the basis for the planning, development, and implementation of business management systems that comply with Federal mandates and requirements, and will produce accurate, reliable, timely, and compliant information for DoD staff. PSAs will define the level of specificity for their Core Business Mission areas. In some cases, the BEA will include separately maintained CBM-specific architecture and requirements.
Business Mission Area	A defined area of responsibility with function and processes that contribute to mission accomplishment.
Business System	An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (10 U. S. C. 2222 (j) (2)) In addition the DODD 8500.1 defines a system as a "set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information."
Business System Modernization Investment	The acquisition or development of a new defense business system; or any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services).
CA Interest	Specific systems or systems supporting specific lines of business that are identified by an CA as being of interest. There is no dollar threshold.
Capability	The ability to execute a specified course of action. It is defined by an operational user and expressed in broad terms in the format of an Initial Capabilities Document (ICD), or a Doctrine, Organization, Training, Material, Personnel, and Facilities (DOTMLPF) change recommendation.
Component	DoD Components are defined to be the Office of the Secretary of Defense, the military departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, the DoD field activities, and all other organizational and operational entities within the DoD.
Core Business Mission	A defined area of responsibility with functions and processes that contribute to mission accomplishment

Term	Definition
Computer Network	The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.
Core System	An existing system, a system in development, or a system beginning the acquisition process that is/will become the Department's solution for a given capability(ies), as designated by the PSA.
DoD Enterprise Systems	Systems that have been identified to become the standard across the Department of Defense
DoD Enterprise Transition Plan	A plan describing: (A) The acquisition strategy for new systems that are expected to be needed to complete the defense business enterprise architecture. (B) A listing of the defense business systems as of December 2, 2002 (known as legacy systems), that will not be part of the objective defense business enterprise architecture, together with the strategy for terminating those legacy systems that provides for reducing the use of those legacy systems in phases. (C) A listing of the legacy systems (referred to in subparagraph (B) that will be a part of the objective defense business systems, together with a strategy for making the modifications to those systems that will be needed to ensure that such systems comply with the defense business enterprise architecture. Each of the strategies *[above]* shall include specific time-phased milestones, performance metrics, and a statement of the financial and non-financial resources needs.
Federated Architecture	An approach for enterprise architecture development that is composed of a set of coherent but distinct entity architectures; the architectures of separate members of the federation. The members of the federation participate to produce an interoperable, effectively integrated enterprise architecture. The federation sets the overarching rules of the federated architecture, defining the policies, practices and legislation to be followed, as well as the inter-federate procedures and processes, data interchanges, and interface standards, to be observed by all members of the federation. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission.
Federation	An organizational entity composed of smaller organizational divisions

Term	Definition
	united to achieve a common goal, within which the smaller divisions retain for themselves control over local matters.
Global Information Grid	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.
Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the an executive agency (DoD). For purposes of the preceding sentence, equipment is used by an executive agency (DoD) or f the equipment is used directly by the DoD or is used by a contractor under a contract with the executive agency (DoD) which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.
Information Technology (IT) Portfolio	A grouping of the IT capabilities, IT systems, IT services, and IT system support services (e.g. IT required to support and maintain systems), management, and related investments required to accomplish a specific functional goal. Decisions to make, modify, or terminate IT investments shall be based on the Global Information Grid (GIG) integrated architecture, mission area goals, risk tolerance levels, potential returns, outcome goals, and performance.
Information Technology (IT) System	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Any Acquisition Category (ACAT) system that meets these criteria, anything categorized as a National Security System (NSS) or a Mission Assurance Category (MAC) level is, by definition, considered to be an IT system. Other types of IT systems include: • DoD-wide, Joint systems • Federal System used by DoD or supported by DoD

Term	Definition

	• DoD System used as a Federal System
	• Multi- System
	• Standard System
	• Major Command Standard System (Echelon 2 or equivalent for Navy and Marine Corps)
	• Below Major Command System (below Echelon 2 or equivalent for Navy and Marine Corps) (e.g., bridges, uniques used at a single site)
	• Data Stores/Data Warehouses
	• Enclaves
	  • Portals (Enterprise)
	  • Automated Information System (AIS) Application

Interim System	An existing system or system in development, as designated by the PSA, that supports the Department for a given capability during a limited period of time. An interim system may have the potential to become part of the core solution.
Legacy System	An existing system that is designated for closure when the capability is absorbed by an interim or core system or if the capability is no longer required.
Major Automated Information System (MAIS)	An MAIS is an Automated Information System (AIS) program that is: 1) designated by the OSD(NII) as an MAIS; or 2) estimated to require program costs in any single year in excess of $32 million (FY 2000 constant dollars) or total program costs in excess of $126 million (FY 2000 constant dollars). MAIS do not include Information Technology (IT) that involves equipment that is an integral part of a weapons system or is an acquisition services program.
Major Defense Acquisition Program (MDAP)	A Department of Defense acquisition program that is not a highly sensitive classified program (as determined by the SECDEF) and that is designated by the SECDEF as a major acquisition program or that is estimated by the SECDEF to require an eventual total expenditure for research, development, test, and evaluation of more than $300M (Based on fiscal year 1990 constant dollars) or an eventual total expenditure for procurement of more than $1.8B based on fiscal year 1990 constant dollars).
Mission Assurance Category 1 (MAC I)	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

Term	Definition
Mission Assurance Category II (MAC II)	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.
Mission Assurance Category III (MAC II)	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of lost of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. **
Modernization Costs	All costs, of any type of funding, incurred to design, develop, implement/deploy and/or functionally enhance/technically upgrade an information technology system. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency and inter-agency services from other Federal agencies. Does not include sustainment costs. Sources, OMB A-11, A-130
National Security Systems (NSS)	Any telecommunications or information system operated by the U.S. Government, the function, operation, or uses of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military and intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications).
Net-Centric Operations and Warfare (NCOW) Reference Model	The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest services, and environment control services), and the enterprise management components. It is also describes a selected set of key standards that shall be needed as the NCOW capabilities of the GIG are realized.
Portal	Provide a single web "location" from which many services and

Term	Definition
	communications systems are accessed. May also be the establishment of a single secure web access point from which applications and information may be distributed. To enable enterprise portal services there must be: Web services, a global directory service, and PKI.
Portfolio Management	The management of selected groupings of IT investments using integrated strategic planning integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investment strategies. The core activities associated with portfolio management are analysis, selection, control, and evaluation.
Special Interest Program	A program may be special interest based on one or more of the following factors: technological complexity; Congressional interest; a large commitment of resources; the program is critical to achievement of a capability or set of capabilities; or the program is a joint program. Exhibiting one or more of these characteristics, however, shall not automatically lead to a 'special interest' designation.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (DODAF). **Sub-system:** A distinct element of a system that can stand alone outside of its system environment **Module:** A distinct element of a system that cannot stand alone outside of its system environment. **Family of Systems:** A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation. **System of Systems:** A set or arrangement of independent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.
Transition Planning	The activities associated with developing the plan and framework for moving from the "As Is" to the "To Be" using strategic plans, Business Capabilities, and architecture information. It incorporates investment management decisions made during the Portfolio Management, PPBE, DAS, and JCIDS processes. It includes the identification of gaps between the "As Is" and the "To Be."

12.0 ACRONYMS

Acronym	Definition
ACAT	Acquisition Category
ADM	Acquisition Decision Memorandum
AIS	Automated Information System
ASD (NII/CIO)	Assistant Secretary of Defense for Networks and Information Integration / CIO
AT&L	Acquisition, Technology and Logistics
BEA	Business Enterprise Architecture
BMA	Business Mission Area
BMMP	Business Management Modernization Program (formerly Financial Management Modernization Program)
BMMP - PEO	Business Management Modernization Program - Program Executive Office
CA	Certification Authority
CBM	Core Business Mission
CDD	Capability Development Document
CIO	Chief Information Officer
CPD	Capabilities Production Document
COCOMS	Combatant Commanders
DAES	Defense Acquisition Executive Summary
DAS	Defense Acquisition System
DBSMC	Defense Business Systems Management Committee
DEPSECDEF	Deputy Secretary of Defense
DITPR	DoD Information Technology Portfolio Repository
DoD	Department of Defense
DODD	Department of Defense Directive
ETP	Enterprise Transition Plan
FCB	Functional Capabilities Board
FM	Financial Management
FMMP	Financial Management Modernization Program (renamed Business Management Modernization Program)
FY	Fiscal Year
GIG	Global Information Grid
HRM	Human Resources Management
IR	Investment Review
IRB	Investment Review Board
IRBWG	Investment Review Board Working Group
IT	Information Technology
ITMA	Information Technology Management Application
JCIDS	Joint Capabilities Integration Development System
JCS	Joint Chiefs of Staff

JFCOM	U.S. Joint Forces Command
MAC I	Mission Assurance Category 1
MAC II	Mission Assurance Category II
MAC III	Mission Assurance Category III
MAIS	Major Automated Information System
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MSSM	Material Supply and Service Management
NDAA	National Defense Authorization Act
NII	Networks and Information Integration
NSS	National Security System
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PA&E	Program Analysis and Evaluation
PCA	Pre-Certification Authority
PEO	Program Executive Office(r)
PKI	Public Key Infrastructure
PSA	Principal Staff Assistant
PfM	Portfolio Management
POC	Point of Contact
SECDEF	Secretary of Defense
TRANSCOM	U.S. Transportation Command
USC	United States Code
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD (P&R)	Under Secretary of Defense for Personnel and Readiness
USD (C)	Under Secretary of Defense (Comptroller)
WSLM	Weapon System Lifecycle Management

APPENDIX A SAMPLE - IRB CHARTER

I. AUTHORITY

10 U. S. C. 2222 as added by Section 332 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375).

II. MISSION/PURPOSE

1. To further advance the development of business operations in support of the Warfighter, and consistent with the aforementioned law, the Investment Review Board (IRB) for XXX is established. This Board will review the planning, design, acquisition, development, deployment, operation, maintenance, modernization, and project cost benefits and risks of all defense business systems for which the respective certification authority is responsible. The Board will make certification recommendations to the Certification Authority.
2. This transformation involves a conscious and sustainable transition to a significantly higher level of performance required to support the warfighter. The overall goal of the IRB is to ensure that the Business Mission Area (BMA) meets the needs and priorities of the Warfighting Mission Area.
3. This Board is the forum to deliberate and recommend to the CA the investments in information systems that will achieve mission and business requirements. Investment review includes assessing the project costs, benefits, and risks associated with the planning, design, acquisition, development, and deployment of systems that support the XXX BMA.

III. ROLES & RESPONSIBILITIES

Working with stakeholders in accordance with the Investment Review Process, dated XXX, the IRB will:

1. Provide investment recommendations to the relevant Certification Authority based on business needs and processes throughout the entire life cycle including design, selection, implementation, management, evaluation, modification, and termination of programs, projects, and systems.

2. Periodically review, but not less than annually, all defense system investments by Core Business Mission Area.

3. Establish compliance criteria for the respective Core Business Mission Area

4. Establish metrics and targets by which to track business transformation progress.

5. Establish an IRB review and approval matrix baselines.

6. Review and recommend certification decisions all defense business system modernizations (new/modifications/enhancements) greater than $1M.

7. Document and report reviews and certifications performed.

8. Provide Components with feedback and status.

9. Sign progress reports to the DBSMC as requested.

IV. MEMBERSHIP

Chairperson is appointed by the CA to represent the XXX Core Business Mission Area.

The Chair will:

Preside at IRB meetings
Approve the agenda and minutes for each meeting, and post information (i.e. portal, website, etc)
Call meetings as required
Establish priorities and strategic direction for the business systems review
Appoint additional members to the IRBs as appropriate
Establish a support activity to coordinate IRB activities utilizing the Rules of Engagement procedures
Coordinate with other IRBs when require, for systems that perform multiple functions and cross business mission areas
Report all business system certifications to DBSMC for final approval

The Board representation consists of the appropriate officials from among the OSD offices, armed forces, combatant commands, the Joint Chiefs of Staff, and defense agencies. Participants in Board matters shall follow all applicable ethics laws and regulations.

Approved: _____
Approval Authority

Appendix B Sample – Component Pre-Certification Authority Designation Letter

MEMORANDUM FOR VICE CHAIR, DBSMC

SUBJECT: System Investment Approval Authority

(Name) is the Pre-Certification Authority for investments over $1 million. He can be reached at (Phone Number) or (Email Address).

(Name) is the approval authority for investments under $1 million. He can be reached at (Phone number) or (Email Address).

Service Secretary or Agency Head

_____

Appendix C Sample – Review and Certification of Economic Viability

MEMORANDUM FOR _____ COMPONENT PCA

SUBJECT: Independent Review and Certification of Economic Viability and Business Case

I have completed review and assessment of the (Name of System's) economic viability and find that the assumptions are valid and the costs and benefits are supportable and fairly represented.

My point of contact is (name) who may be reached at (phone number) or (email address).

Independent Cost Activity
Signature (as designated)

Appendix D Sample – Component Pre-Certification Letter

MEMORANDUM FOR _____ INVESTMENT REVIEW BOARD CHAIRMAIN

SUBJECT: Pre-certification of Compliance

1. The Program Manager of the (Name of defense business system modernization) requests _____ (authority to obligate $__ in funding). This _____ (modernization effort) is required to_____*(summarize how it will improve performance, improve warfighter support, satisfy a mandate, law, policy, regulation, or provide a critical capability)*

2. I have determined this _____ (system modernization) is consistent with the ____ (Component Name) Business Systems Transition Plan and compliant with the _____ (Component Name or DoD Enterprise) architecture. An Economic Viability Analysis was completed and reviewed by the program's cost authority who concurs with the economic viability analysis. *(Economic analysis is only required for new acquisitions)*

3. The information contained in the Department of Defense Information Technology Portfolio Repository, DIPTR, for this system is verified to be complete and accurate as of _____ (date).

4. Based on my review, I have concluded that this business systems modernization:
(insert one of the following A, B or C below)
(A) is in compliance with the enterprise architecture;
(B) is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or
(C) is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect.

I recommend the _____ (Human Resources Management, Financial Management, Weapon System Lifecycle Management, Materiel Supply & Service Management, or Real Property & Installation Lifecycle Management) Investment Review Board certify to the Defense Business Systems Management Committee (DBSMC) approval of this request.

A completed certification questionnaire and Economic Viability Analysis are forwarded for your review.

My point of contact for questions about this submission, is (Name) who may be reached at (Phone Number) or email at (Email Address).

Component Headquarters PCA

Appendix E Standard Set of IRB Criteria for Certification

Basic System Information	**Verification**
Points of Contact	
Which Core Business Mission Area is primary?	Factual Data
Which Core Business Mission Area(s) have interest?	Factual Data
Which Component is Sponsoring the System?	Factual Data
Who is the Component PCA?	Factual Data
Who is the PCA POC? What is the POC's phone number?	Factual Data
Who is the Milestone Decision Authority (MDA)?	Factual Data
Description	
What is the Program/Initiative Title?	Factual Data
What is the Program/Initiative Acronym?	Factual Data
Is the system registered in a DoD repository?	Factual Data
(e.g., DoD IT Registry, ITMA, DITPR)	Factual Data
What is the registry #?	
Is this system a Core, Interim or Legacy system?	Factual Data
Is this a Joint program/initiative?	Factual Data
Which tier is the enhancement/modernization?	Factual Data
Funding/Budget	
Provide the schedule, milestones, and funding over the FYDP. Account for all funds by appropriation, proposed in that fiscal year budget for the system, including O&M (or Steady State) and Development, Modernization and Enhancement. Provide information by FY, including prior years.	Factual Data
What is the amount of the modernization/enhancement to be certified? Provide amount by FY.	Factual Data
Is the Program/Initiative fully funded through the FYDP?	Factual Data
What is the System Lifecycle Stage?	Factual Data
What is the Acquisition Category?	Factual Data
Certification Request	
Date submitted for Certification.	Factual Data
Date PCA certified.	Factual Data
What event requires Certification? • Milestone Approval • Authority to Obligate	Factual Data
Other (explain)	Factual Data
What is the date modernization/enhancement funds would be obligated?	Factual Data
Describe the modernization/enhancement.	Description
Amplifying discussion (as required).	Discussion

Justification

What COCOM 57/129, DoD Enterprise, or Component specific requirement(s) does this initiative address?	Checklist
Would denial of this modernization/enhancement request adversely affect DoD operations? Please describe.	Description
If Program/Initiative is less-than-MAIS, has the agency component independent cost review authority reviewed and validated the economic viability? • Attach a copy of the Component's economic viability analysis. • Attach a copy of the independent cost review authority validation.	Attachments
Provide program overview/description.	Attachment
Does this modernization/enhancement help transform the Department's business processes? Please explain.	Explanation
Could another existing system or an e-GOV initiative, be adapted or used to resolve the requirement?	Checklist
Does it duplicate an e-GOV initiative? If so, justify.	Checklist/just
Are there significant risks associated with this system/program that may affect the successful deployment and operation of this system? If so, provide mitigation strategy.	Review Strategy
Identify any GAO, DoDIG, other audit findings, or material weaknesses and the planned resolution.	Review Resolution
Program/Initiative aligned to applicable Policies, Laws and Regulations?	Certifications

(NOTE: if the system is not certified for any of the below, provide justification.)

- Is the Program/Initiative DITSCAP compliant? If not DITSCAP Compliant, has system received Interim Approval to Operate (IATO)?
- Is the Program required to complete the Annual Federal Information Security Management Act (FISMA) Report? Has this report been completed or is it in progress? If not, justify.
- Is Program/Initiative Compliant with the Clinger-Cohen Act (CCA)? If not, justify.
- If a financial management or mixed system, is the Program/Initiative Federal Financial Management Improvement Act (FFMIA) Compliant? If "No" has an FFMIA Compliance Plan been prepared?
- Is the program Health Insurance Portability and Accountability Act (HIPPA) compliant?
- Is the program compliant with the Privacy Act of 1974?
- Does the System have a current, DoDAF compliant Architecture? If not justify.
- Is the Program/Initiative schedule consistent with the Net Centric requirement? If not, justify.
- Are there other rules or mandates that may influence the need for this program? Please describe.

Transition Plan (These criteria will be effective beginning October 1, 2005.)

Is the business system modernization initiative identified in the DoD or Component Transition Plan? If not in the Transition Plan, is the initiative critical to national security/safety? How? Provide supporting documentation.	Compare w/ Transition Plan
Are there programmatic/technical dependencies with other systems? • Identify dependencies.	Cross-reference with other systems
Identify systems or system modules eliminated (with sunset dates).	Trans Plan

Architecture

Identify the activities or processes (DoD enterprise and/or Component) supported by this system modernization or enhancement initiative. Are these activities or processes aligned with the activities listed in the DoD BEA (or Component activities aligned to the BEA)? Provide AV-1, TV-1, and OV-5.	Verify Alignment
Identify capabilities/functions encompassed by the Program/Initiative and define how they enable the supported operational activities.	Checklist
Is the Program/Initiative required to achieve a BEA objective? If yes, identify the BEA objective(s).	Checklist
Is the Program/Initiative compliant with the Business Enterprise Architecture and the Component architecture? If not, justify.	Checklist Justification
Does this initiative comply with the applicable technical environment established by the DoD BEA TV-1? If not, and this initiative is part of the BEA, does its migration plan reflect future compliance.	Review TV-1/ Migration Plan
Are the system interfaces identified and schedules aligned?	Discussion

Certification Results

CA Certification Decision.
Date of CA decision.
DBSMC Approval Decision.
Date of DBSMC decision.
Certification/Approval rationale.
- BEA Compliance
- National security requirement
- Avoid adverse operational impact

Any comments relating to the actions, approval or rejection of the system review/certification.
(Comments are mandatory when the review outcome is other than “Certified”)